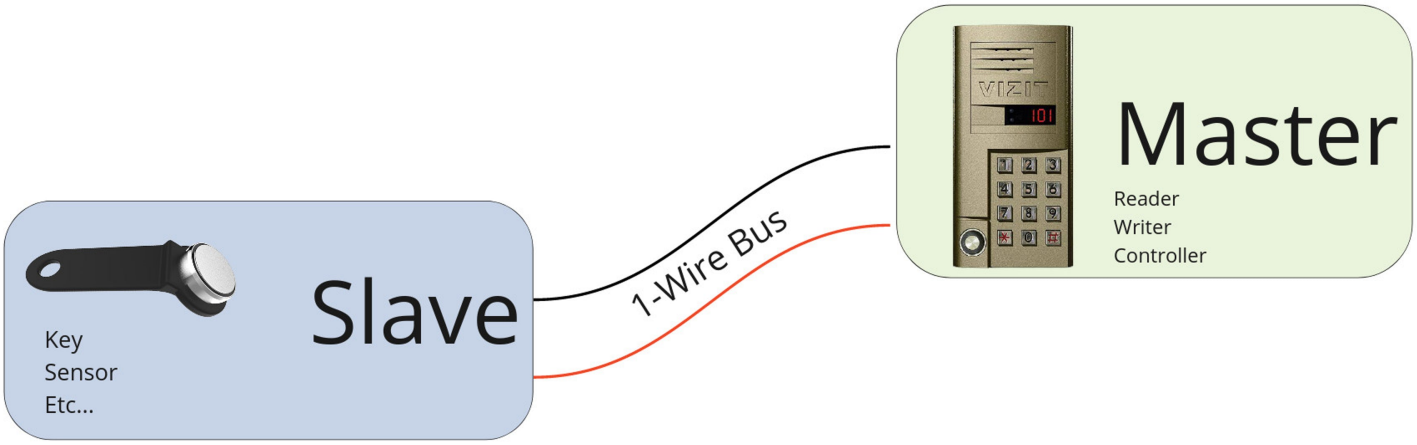
16min

Протокол 1-Wire



Протокол 1-wire всегда имеет главное устройство Master и ведомое Slave

Домофонные ключи используют всего один контакт на приём и передачу данных, используя протокол 1-Wire в режиме Master-Slave. Устройство Master всегда инициирует общение, а Slave следует его указаниям. При контакте ключа (Slave) с домофоном (Master) чип внутри ключа получает питание от домофона. После чего происходит инициализация ключа и домофон запрашивает его ID.

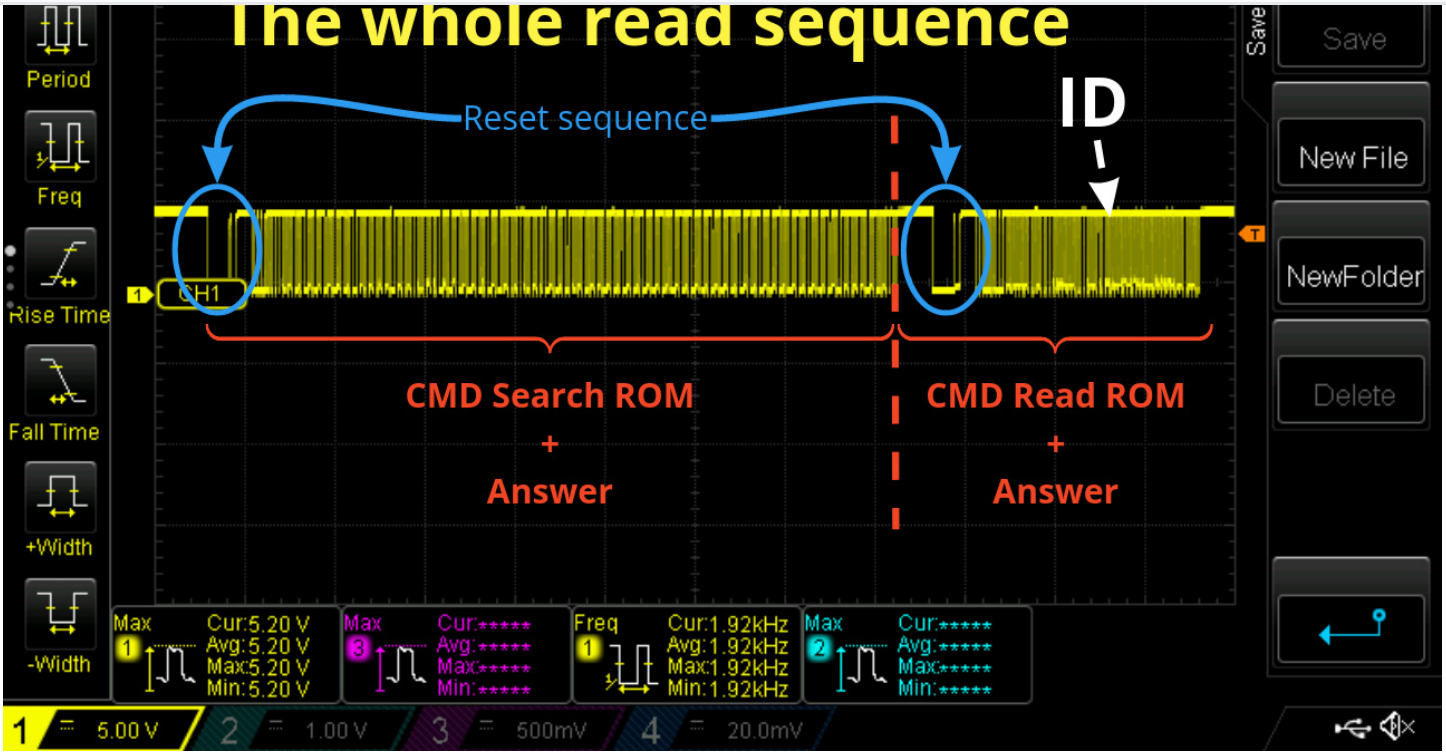
Флиппер выступает в роли считывателя, то есть работает как Master. При эмуляции ключа Флиппер прикидывается ключом, то есть работает в режиме Slave.

Смотрим на 1-Wire через осциллограф

Линия передачи устроена по принципу «монтажного И» и может иметь одно из двух состояний: логический “0” и логическая “1”. Устройства (ключи и домофон) имеют внутренние транзисторы, которые в нужное время подтягивают линию к нулю. Вся линия передачи переходит в состояние логического “0”, если любое из устройств перевело ее в нуль, т.е. если домофон перетянул линию в нуль — ключ об этом узнает, и наоборот.

С помощью перетяжек напряжения и удержания уровней 1-wire имеет 4 примитива для работы на шине:

1. импульс сброса (RESET)
2. импульс присутствия (PRESENCE)
3. отправка бита 0



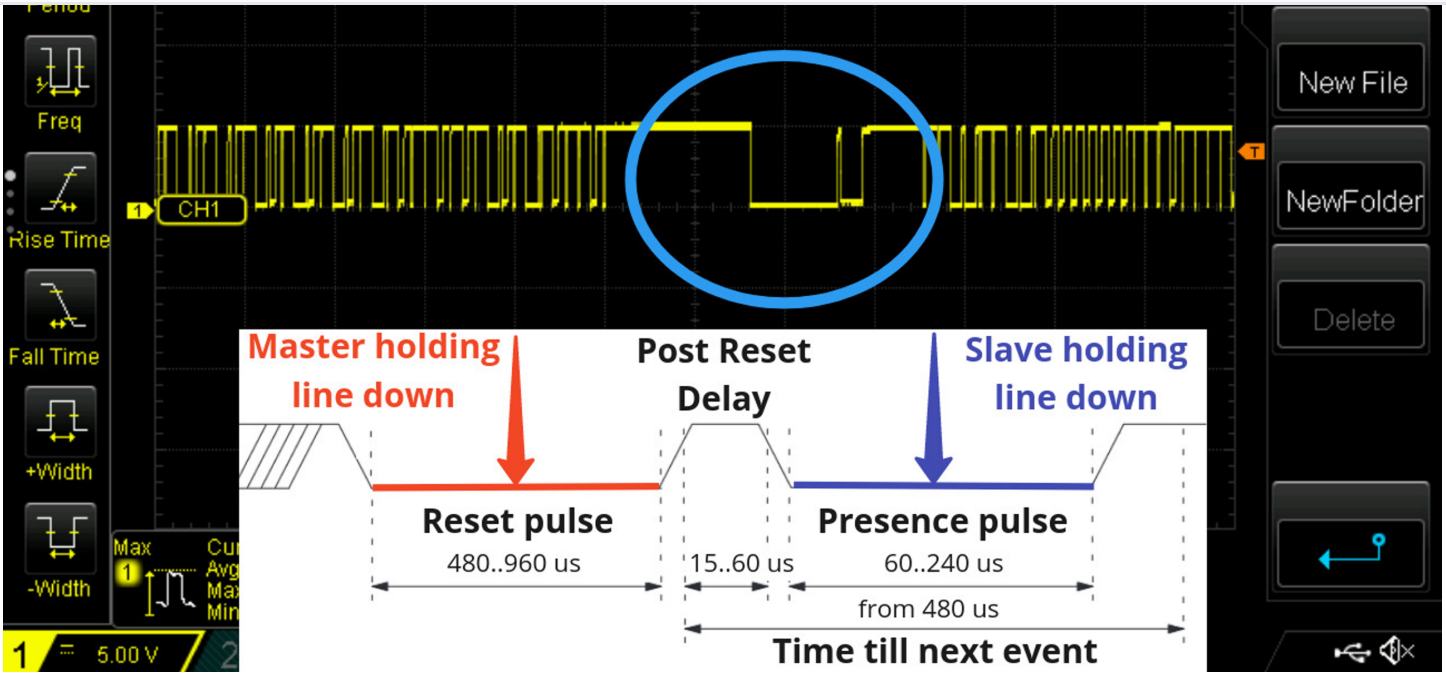
Чтение ключа Dallas на Flipper состоит из команд Search ROM и Read ROM. Каждая команда имеет Reset sequence

Чтение ключа на Flipper Zero устроено так: командой поиска проверяется наличие ключа, а затем происходит чтение ID. Это сделано, чтобы избежать случайных совпадений с другими ключами Cyfral/Metakom, тайминги которых могут случайно совпасть с требуемыми.

На осциллограмме виден длинный сигнал из 2 команд, где каждая состоит из:

- Инициализации команды:
  - Импульс сброса
  - Импульс присутствия
- Передачи команды для Slave
- Ответа Slave на принятую команду

Инициализация команды



Reset sequence — инициализация команды. Состоит из Импульса Сброса и Импульса Присутствия. Импульс Сброса — уровень опускает Master. Импульс Присутствия — уровень опускает Slave

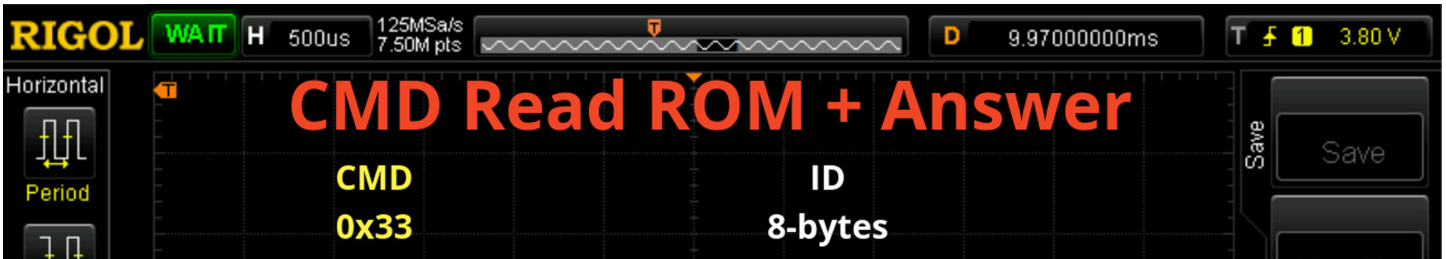
Инициализация (reset sequence) состоит из двух импульсов:

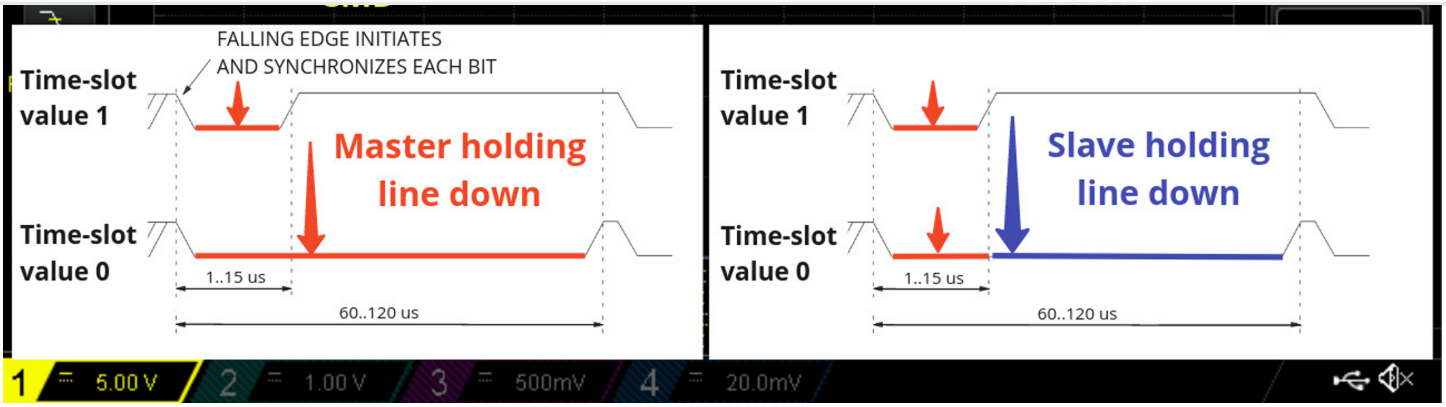
1. Импульс Сброса (Reset pulse)
2. Импульса Присутствия (Presence pulse)

Для Импульса Сброса — линию к земле подтягивает Master (домофон).
Для Импульса Присутствия — линию к земле подтягивает Slave (ключ).

Некоторые домофоны не подают импульс сброса, так как отсутствие контакта между ключом и домофоном и есть сигнал сброса.

Передача команды и получение ответа





Команда чтения ID с ответом. Тайм-слот бита информации состоит из 2 участков: синхронизации и значения бита. В КОМАНДАХ за уровни напряжения на обоих участках отвечает Master. В ОТВЕТЕ на команду чтения за синхронизацию отвечает Master, за значение бита отвечает Slave

После инициализации команды происходит обмен информацией:

- отправка команды для Slave
- ответ Slave на команду

Обмен информацией ведется тайм-слотами: один тайм-слот для обмена одним битом информации. Данные передаются бит за битом, начиная с младшего бита младшего байта.
Синхронизация Master и Slave происходит в одно действие: Master (домофон) подтягивает линию к низкому уровню. Далее Master или Slave измеряет напряжение на линии и записывает бит информации (Master — при чтении ключа, Slave — при записи ключа). Временные диапазоны для команд чтения и записи одинаковы.

Каждый тайм-слот синхронизируется независимо, поэтому передача информации может приостанавливаться, не вызывая ошибок. Важно, что все сигналы имеют конкретные временные диапазоны, которые обязательно должны быть соблюдены! Бывает, что производители домофонов упарываются, и используют свои временные задержки.

Еще у iButton есть режим Overdrive, в котором временные задержки